IQI 04, Seminar 3

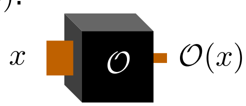
Produced with pdflatex and xfig

- Oracles
- The Classical Parity Problem.
- Quantum Oracles.
- The Quantum Parity Problem.
- Gate Set Limitations.
- Universality.

E. "Manny" Knill: knill@boulder.nist.gov

Classical Oracles

- A classical oracle $\mathcal{O}$ is a device that takes an input x and outputs an answer $\mathcal{O}(x)$.



Examples:

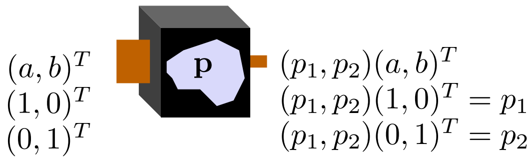
- $\mathcal{O}_1(x) = 1$ if x is a true statement about numbers, $\mathcal{O}_1(x) = 0$ otherwise.
- $\mathcal{O}_2(x) = 1$ if x is a satisfiable logical statement, $\mathcal{O}_2(x) = 0$ otherwise.

  ...Oracles can be used to add computational power.
- $\mathcal{O}_3(x)$ computes an unknown parity of x. Determine the parity.

...Oracles can act as black boxes to be analyzed.

Parity Oracles

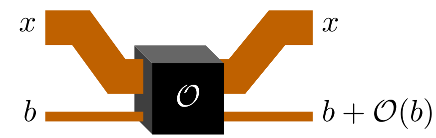
- Bit strings may be identified with 0-1 vectors.
  Example: $0110 \leftrightarrow (0,1,1,0)^T$
- The parity of bitstring $\mathbf{s}$ is the number of 1's in $\mathbf{s}$ modulo 2.
  Example: $P(1101) = (1,1,1,1)(1,1,0,1)^T = 3 \bmod 2 = 1$
  ...computations with 0-1 entities are modulo 2.
- Parity of a substring.
  Examples:
  $P_{\mathbf{p}}(\mathbf{s}) = \mathbf{p}\cdot\mathbf{s}$
- A parity oracle.



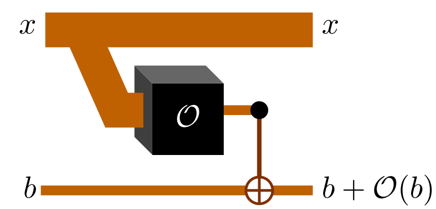
How many "queries" does it take to learn $\mathbf{p}$?

Reversible Oracles

- Reversible oracles add the answer to a register.



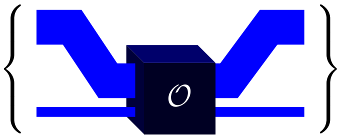
- Simulation, using a standard oracle.



- Is the simulation equivalent to a reversible oracle?

Quantum Oracles

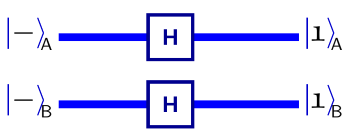
- A Quantum Oracle is the linear extension of a classical reversible oracle.

$\sum_{x,b}\alpha_{x,b}|x\rangle_{\mathsf{I}}|b\rangle_{\mathsf{O}}$  $\sum_{x,b}\alpha_{x,b}|x\rangle_{\mathsf{I}}|b+\mathcal{O}(x)\rangle_{\mathsf{O}}$

- Quantum oracles versus classical reversible oracles?
  - Does it help to use a quantum computer to analyze a classical reversible oracle?

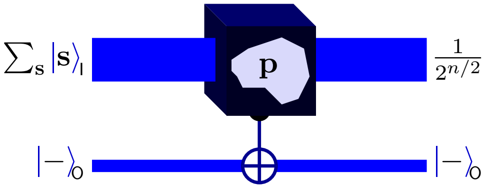
The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.
- Solution in two tricks. Def.: $\begin{cases}|+\rangle = \frac{1}{\sqrt{2}}(|\mathfrak{o}\rangle+|\mathfrak{1}\rangle)\\ |-\rangle = \frac{1}{\sqrt{2}}(|\mathfrak{o}\rangle-|\mathfrak{1}\rangle)\end{cases}$
  1. Parity and the Hadamard basis.
     - Which logical states $|\mathfrak{ab}\rangle_{\mathsf{AB}}$ have a minus sign in
       $|+\rangle_{\mathsf{A}}|+\rangle_{\mathsf{B}},\ |+\rangle_{\mathsf{A}}|-\rangle_{\mathsf{B}},\ |-\rangle_{\mathsf{A}}|+\rangle_{\mathsf{B}},\ |-\rangle_{\mathsf{A}}|-\rangle_{\mathsf{B}}$?
     - Ans.: States with odd parity w.r.t. the $|-\rangle$-qubits.
     - Are these states distinguishable?



The Quantum Parity Problem

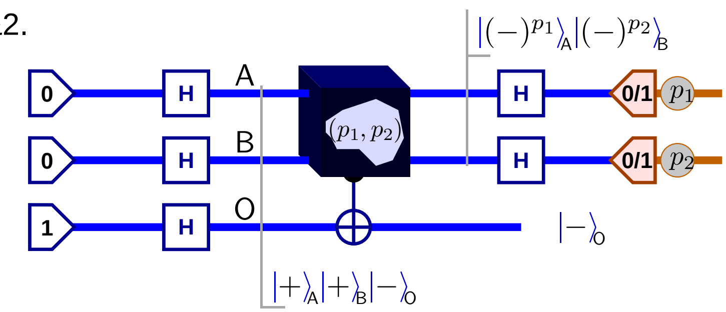
- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.
- Solution in two tricks.
  2. Sign kickback for oracles with one-bit answers.

$\frac{1}{2^{n/2}}\sum_{\mathbf{s}}|\mathbf{s}\rangle_{\mathsf{I}}$  $\frac{1}{2^{n/2}}\sum_{\mathbf{s}}(-1)^{\mathbf{p}\cdot\mathbf{s}}|\mathbf{s}\rangle_{\mathsf{I}}$

- $|-\rangle$ is an eigenstate of $\mathbf{not}$ with eigenvalue -1.

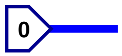
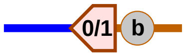
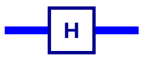
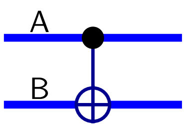
The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.
- Solution in two tricks.
  1.&2.



- One query suffices for solving the n-qubit parity problem.

Summary of Gates Introduced So Far

Gate picture	Symbol	Matrix form
	$\mathbf{prep}(0)$	
	$\mathbf{meas}(Z{\mapsto}b)$	
	$\mathbf{not}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
	$\mathbf{sgn}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
	$\mathbf{had}$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
	$\mathbf{cnot}^{(\mathsf{AB})}$	$\begin{array}{c} \\ \lvert 00\rangle_{AB} \\ \lvert 01\rangle_{AB} \\ \lvert 10\rangle_{AB} \\ \lvert 11\rangle_{AB} \end{array}\begin{array}{c} \lvert 00\rangle_{AB}\ \lvert 01\rangle_{AB}\ \lvert 10\rangle_{AB}\ \lvert 11\rangle_{AB} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$

Properties of Reversible Gates

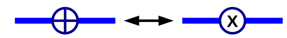
- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...
- Conjugating V by U gives $U^{-1}.V.U$.

  - Applications: Network rearrangements.

Error effect determination.

Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn}$, $\mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}$.
- $\mathbf{sgn}$ and $\mathbf{not}$ conjugated by $\mathbf{had}$.

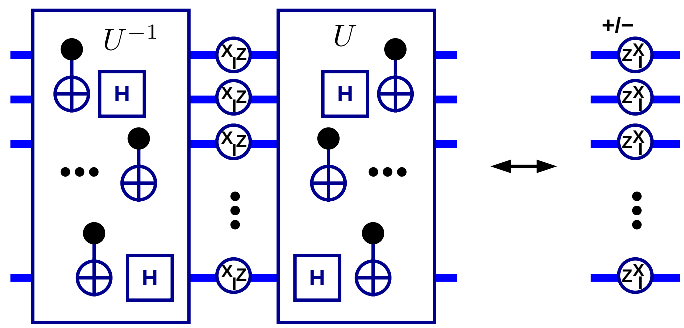
$$\mathbf{had}^{-1}.\mathbf{sgn}.\mathbf{had} = \mathbf{not},\ \ \mathbf{had}^{-1}.\mathbf{not}.\mathbf{had} = \mathbf{sgn}.$$

- $\mathbf{sgn}$ and $\mathbf{not}$ conjugated by $\mathbf{cnot}$.

$$\begin{aligned} \mathbf{cnot}^{(\mathsf{AB})-1}.\mathbf{not}^{(\mathsf{B})}.\mathbf{cnot}^{(\mathsf{AB})} &= \mathbf{not}^{(\mathsf{B})}, \\ \mathbf{cnot}^{(\mathsf{AB})-1}.\mathbf{sgn}^{(\mathsf{A})}.\mathbf{cnot}^{(\mathsf{AB})} &= \mathbf{sgn}^{(\mathsf{A})}, \\ \mathbf{cnot}^{(\mathsf{AB})-1}.\mathbf{not}^{(\mathsf{A})}.\mathbf{cnot}^{(\mathsf{AB})} &= \mathbf{not}^{(\mathsf{A})}.\mathbf{not}^{(\mathsf{B})}, \\ \mathbf{cnot}^{(\mathsf{AB})-1}.\mathbf{sgn}^{(\mathsf{B})}.\mathbf{cnot}^{(\mathsf{AB})} &= \mathbf{sgn}^{(\mathsf{A})}.\mathbf{sgn}^{(\mathsf{B})} \end{aligned}$$

Preservation of Products of "Flips"

- Products of $\mathbf{not}$ and $\mathbf{sgn}$ are preserved under conjugation by operators composed of $\mathbf{cnot}$'s and $\mathbf{had}$'s.



  - What is the power of this gate set?

Physically Allowed Reversible Operators

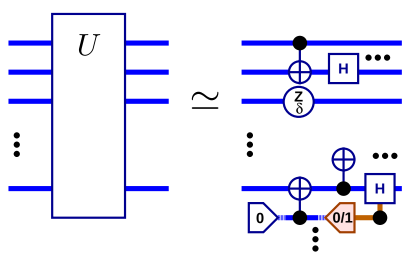
- Define an operator U by linear extension of
  $$U|x\rangle_{\mathsf{S}} = \sum_y u_{yx}|y\rangle_{\mathsf{S}}$$
  - To be well-defined, $U|x\rangle_{\mathsf{S}}$ must be a state:
    $$\sum_y |u_{yx}|^2 = 1.$$
  - U's linear extension must preserve states.
    Consider $U\frac{1}{\sqrt{2}}(|x\rangle_{\mathsf{S}} + e^{i\phi}|z\rangle_{\mathsf{S}}) = \sum_y \frac{1}{\sqrt{2}}(u_{yx} + e^{i\phi}u_{yz})|y\rangle_{\mathsf{S}}$.
    Hence $\sum_y \bar{u}_{yx}u_{yz} = 0$.
- U is *unitary*. In matrix form with $x \in \{1, 2, \ldots, N\}$:

$$\overset{U^\dagger}{\begin{pmatrix} \bar{u}_{11} & \bar{u}_{21} & \ldots & \bar{u}_{N1} \\ \bar{u}_{12} & \bar{u}_{22} & \ldots & \bar{u}_{N2} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{u}_{1N} & \bar{u}_{2N} & \ldots & \bar{u}_{NN} \end{pmatrix}} \overset{U}{\begin{pmatrix} u_{11} & u_{12} & \ldots & u_{1N} \\ u_{21} & u_{22} & \ldots & u_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ u_{N1} & u_{N2} & \ldots & u_{NN} \end{pmatrix}} = \overset{\mathbb{1}}{\begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}}$$

- Should every unitary operator be implementable?

Universality for Gate Sets

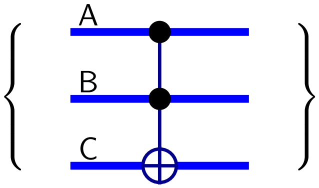
- Should every unitary operator be implementable?
- A set of gates is *universal* if every unitary n-qubit can be implemented with a network.



- Other notions of universality:
  - Allow use of ancillas and measurements.
  - Allow approximation to within arbitrarily small error.

Locality Constraints on Gate Sets

- Can any n-qubit unitary operator be a gate?
  - "Good" gates are physically realizable in one step.
  - Locality: Elementary gates act on at most three qubits.
    The Toffoli gate: $\mathbf{c}^2\mathbf{not}^{(\mathsf{ABC})} = \underline{\textbf{if}}\ \mathsf{A}\&\mathsf{B}\ \underline{\textbf{then}}\ \mathbf{not}^{(\mathsf{C})}$.

$|\mathfrak{abc}\rangle_{\mathsf{ABC}}$


$|\mathfrak{ab}(c + \mathfrak{a}\cdot\mathfrak{b})\rangle_{\mathsf{ABC}}$

  - Discreteness: Finite gate sets are preferred.
  - Fault tolerance: Elementary gates should be experimentally verifiable and readily made stable.
- ...but do investigate other gate sets.

Contents

References

[1] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26:1411–1473, 1997.

[2] L. K. Grover. Quantum computers can search arbitrarily large databases by a single query. *Phys. Rev. Lett.*, 79:4709–4712, 1997.

[3] D. A. Meyer. Sophisticated quantum search without entanglement. *Phys. Rev. Lett.*, 85:2014–2017, 2000.